



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/790,082	03/02/2004	Takeo Yoshida	118918	2490
25944 7590 04/03/2007 OLIFF & BERRIDGE, PLC P.O. BOX 19928 ALEXANDRIA, VA 22320			EXAMINER LOUIE, OSCAR A	
			ART UNIT	PAPER NUMBER
			2109	
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		04/03/2007	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/790,082

Applicant(s)

YOSHIDA, TAKEO

Examiner

Oscar A. Louie

Art Unit

2109

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 13 April 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>04/06; 03/04</u> | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2109

DETAILED ACTION

This first non-final action is in response to the original filing of 03/02/2004. Claims 1-13 are pending and have been considered as follows.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 10 is rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for a connection server apparatus for being connected to a client apparatus, does not reasonably provide enablement for using a single definition for creating a number of objects. The apparatus in this claim consists of a single element: "a unit for receiving an address of the client apparatus to be connected from the authentication server, allowing communication from the address for a predetermined period, and transmitting to the authentication server information indicating that the connection server is shifted to a connection wait state", and thus is interpreted as a single means claim under MPEP 2164.08(a).

"A single means claim, i.e., where a means recitation does not appear in combination with another recited element of means, is subject to an undue breadth rejection under 35 U.S.C. 112, first paragraph. In re Hyatt, 708 F.2d 712, 714-715, 218 USPQ 195, 197 (Fed. Cir. 1983) (A single means claim which covered every conceivable means for achieving the stated purpose was held nonenabling for the scope of the claim because the specification disclosed at most only

Art Unit: 2109

those means known to the inventor.). When claims depend on a recited property, a fact situation comparable to Hyatt is possible, where the claim covers every conceivable structure (means) for achieving the stated property (result) while the specification discloses at most only those known to the inventor."

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-10 & 12 are rejected under 35 U.S.C. 102(b) as being anticipated by

Subramaniam (US-6081900-A).

Claim 1:

Subramaniam discloses a network connection system comprising,

- "a client apparatus" [Fig 1].
- "an authentication server" (i.e. "the target server would generally check user permissions against access control lists associated with the data, or take other steps to make sure the requesting user is entitled to access the requested data before providing that data") [column 6 lines 52-56].
- "a connection server" (i.e. "the target server 104 determines that the request came from outside the security parameter") [column 6 lines 48-49].

Art Unit: 2109

- “a retention unit for storing second connection authentication information prepared on the basis of first connection authentication information used in the connection server” (i.e. “the target server”) [column 6 line 52].
- “a first unit for acquiring user identification information from the client apparatus and a client address when the first unit receives a connection request from the client apparatus” (i.e. “the external client 112 requests access to data which is stored on the target server... checking the IP address from which the request was made, communicating with the firewall software, or other familiar means”) [column 6 lines 42-48].
- “a second unit for transmitting the acquired client address to the connection server having the connection server address associated with the second connection authentication information and transmitting the connection server address to the client apparatus, which has transmitted the connection request” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].
- “a third unit for transmitting the second connection authentication information to the authentication server as the user identification information together with the connection request” (i.e. “the external client”) [column 6 lines 42-43].
- “a fourth unit for receiving the connection server address from the authentication server” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].

Art Unit: 2109

- “a fifth unit for transmitting the first connection authentication information to the connection server having the received connection server address” (i.e. “the external client”) [column 6 lines 42-43].
- “a sixth unit for receiving connection from the client address, which has been received from the authentication server” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].
- “a seventh unit for performing an authentication process by using the first connection authentication information transmitted from the client address” (i.e. “the target server would generally check user permissions against access control lists associated with the data, or take other steps to make sure the requesting user is entitled to access the requested data before providing that data”) [column 6 lines 52-56].

Claim 2:

Subramaniam discloses a network connection system as in Claim 1 above further comprising,

- “the second connection authentication information is a message digest of the first connection authentication information” (i.e. “a user name and password, the authentication information may include certificates, tokens, public keys, and/or data from authentication tools such as biometric scans, voice prints, retinal scans, fingerprint scans, magnetic card reader results, and so on. A wide variety of suitable authentication information is familiar to those of skill in the art”) [column 12 lines 40-46].

Art Unit: 2109

Claim 3:

Subramaniam discloses an authentication server for being connected to a client apparatus and a connection server comprising,

- “a retention unit for storing second connection authentication information prepared on the basis of first connection authentication information used in the connection server while associating the second connection authentication information with a connection server address” (i.e. “the target server”) [column 6 line 52].
- “a first unit for acquiring user identification information from the client apparatus and a client address when the first unit receives a connection request from the client apparatus” (i.e. “the target server would generally check user permissions against access control lists associated with the data, or take other steps to make sure the requesting user is entitled to access the requested data before providing that data”) [column 6 lines 52-56].
- “a second unit for transmitting the acquired client address to the connection server having the connection server address associated with the second connection authentication information and transmitting the connection server address to the client apparatus, which has transmitted the connection request” (i.e. “the target server 104, this involves receiving a request during a step 200...By checking the IP address from which the request was made, communicating with the firewall software, or other familiar means, the target server 104 determines that the request came from outside the security parameter”) [column 6 lines 44-49].

Art Unit: 2109

Claim 4:

Subramaniam discloses a client apparatus for being connected to an authentication server and a connection server comprising,

- “a connection request unit for transmitting a connection request and second connection authentication information prepared on the basis of first connection authentication information used in the connection server to the authentication server” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].
- “a unit for receiving a connection server address from the authentication server to transmit the first connection authentication information to the connection server address” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].

Claim 5:

Subramaniam discloses a connection server for being connected to an authentication server and a client apparatus comprising,

- “a control unit for receiving a client address from the authentication server and allowing connection from the client address” (i.e. “the target server 104, this involves receiving a request during a step 200...By checking the IP address from which the request was made, communicating with the firewall software, or other familiar means, the target server 104

Art Unit: 2109

determines that the request came from outside the security parameter”) [column 6 lines 44-49].

- “an authentication unit for receiving authentication information from the client apparatus having the client address, which is allowed the connection, to perform an authentication process by using the authentication information” (i.e. “the target server would generally check user permissions against access control lists associated with the data, or take other steps to make sure the requesting user is entitled to access the requested data before providing that data”) [column 6 lines 52-56].

Claim 6:

Subramaniam discloses a network connection system comprising,

- “a client apparatus” [Fig 1].
- “an authentication server” (i.e. “the target server would generally check user permissions against access control lists associated with the data, or take other steps to make sure the requesting user is entitled to access the requested data before providing that data”) [column 6 lines 52-56].
- “a connection server” (i.e. “the target server 104 determines that the request came from outside the security parameter”) [column 6 lines 48-49].
- “a retention unit for storing a first encrypted user name and a first encrypted password which are encrypted by a first encryption method, while associating a connection server address with the first encrypted user name and the first encrypted password” (i.e. “the target server”) [column 6 line 52].

- “a first unit for acquiring the first encrypted user name and the first encrypted password as identification information for identifying a user of the client apparatus, and a client address when the first unit receives a connection request from the client apparatus” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].
- “a second unit for transmitting the acquired client address to the connection server address associated with the user identification information when the retention unit stores the user identification information, receiving from the connection server information indicating that the connection server is shifted to a connection wait state, and transmitting the connection server address to the client apparatus, which issues the connection request” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].
- “a third unit for transmitting to the authentication server the first encrypted user name and the first encrypted password, which are encrypted by the first encryption method, together with the connection request” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].

Art Unit: 2109

- “a fourth unit for receiving the connection server address from the authentication server, and transmitting to the received connection server address a second encrypted user name and a second encrypted password, which are generated by encrypting a user name and a password, which are input by the user, by a second encryption method” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].

Claim 7:

Subramaniam discloses an authentication server for being connected to a client apparatus and a connection server comprising,

- “a retention unit for storing a user name and a password, which are encrypted by a predetermined method, while the user name and the password are associated with a connection server address” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].
- “a first unit for acquiring the encrypted user name and the encrypted password as identification information for identifying a user of the client apparatus, and a client address when the first unit receives a connection request from the client apparatus” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to

Art Unit: 2109

the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].

- “a second unit for transmitting the acquired client address to the connection server address associated with the user identification information when the retention unit stores the user identification information, receiving from the connection server information indicating that the connection server is shifted to a connection wait state, and transmitting the connection server address to the client apparatus, which issues the connection request” (i.e. “the target server 104, this involves receiving a request during a step 200...By checking the IP address from which the request was made, communicating with the firewall software, or other familiar means, the target server 104 determines that the request came from outside the security parameter”) [column 6 lines 44-49].

Claim 8:

Subramaniam discloses a client apparatus for being connected to an authentication server and a connection server comprising,

- “a connection request unit for transmitting to the authentication server a user name and a password, which are encrypted by a first encryption method, together with a connection request” (i.e. “the external client”) [column 6 lines 42-43].
- “a unit for receiving a connection server address from the authentication server, encrypting a user name and a password, which are input by a user, by a second encryption method, and transmitting the user name and the password, which are encrypted by the second encryption method, to the received connection server address” (i.e. “The user enters a user name and a corresponding password in fields shown on the

Art Unit: 2109

login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].

Claim 9:

Subramaniam discloses a client apparatus for being connected to an authentication server and a connection server as in Claim 8 above further comprising,

- “a retention unit for storing local authentication information, which is previously supplied from the connection server, as information associating unique information of the client apparatus with at least one of the user name and the password” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].
- “a local authentication unit for generating the unique information upon receiving inputting the user name and the password by the user, references the local authentication information to authenticate the user by judging whether or not at least one of the received user name and the received password is associated with the generated unique information” (i.e. “If the username and password are validated by the authentication system, the border server 106 so notifies the user, and the user is then granted access to secure network 100 data as described herein”) [column 8 lines 53-57].

Art Unit: 2109

- “the connection request unit transmits to the authentication server the user name and the password, which are encrypted by the first method, together with the connection request only when the local authentication unit authenticates the user” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].

Claim 10:

Subramaniam discloses a connection server for being connected to a client apparatus,

- “a unit for receiving an address of the client apparatus to be connected from the authentication server, allowing communication from the address for a predetermined period, and transmitting to the authentication server information indicating that the connection server is shifted to a connection wait state” (i.e. “the external client 112 requests access to data which is stored on the target server... checking the IP address from which the request was made, communicating with the firewall software, or other familiar means”) [column 6 lines 42-48].

Claim 12:

Subramaniam discloses a connection method using a network connection system including a client apparatus, an authentication server, and a connection server comprising,

- “storing by the authentication server second connection authentication information prepared on the basis of first connection authentication information used in the connection server while associating the second connection authentication information

with a connection server address” (i.e. “the servers 104, 106 may also be configured by those of skill in the art in a wide variety of ways to operate as Internet servers, as intranet servers, as proxy servers, as directory service providers or name servers, as software component or other object servers, or as a combination thereof”) [column 5 lines 44-49].

- “transmitting by the client apparatus to the authentication server the second connection authentication information as user identification information together with a connection request” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].
- “acquiring the user identifying information from the client apparatus and client address when the authentication server receives the connection request from the client apparatus” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].
- “transmitting the acquired client address to the connection server identified by the connection server address associated with the second connection authentication information when the user identification information meets the second connection authentication information” (i.e. “the external client 112 requests access to data which is stored on the target server... checking the IP address from which the request was made,

communicating with the firewall software, or other familiar means”) [column 6 lines 42-48].

- “transmitting the connection server address to the client apparatus, which issues the connection request” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].
- “receiving by the client apparatus the connection server address from the authentication server” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].
- “transmitting by the client apparatus the first connection authentication information to the received connection server address” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].
- “receiving by the connection server connection from the client address received from the authentication server” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].
- “performing an authentication process by using the first connection authentication information transmitted from the client address” (i.e. “The user enters a user name and a

corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 11 & 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Subramaniam (US-6081900-A).

Claim 11:

Subramaniam discloses a network connection system apparatus comprising,

- “a client apparatus” [Fig 1].
- “an authentication server for supplying information guiding a connection destination to the client apparatus” (i.e. “the target server would generally check user permissions against access control lists associated with the data, or take other steps to make sure the requesting user is entitled to access the requested data before providing that data”) [column 6 lines 52-56].
- “a connection server” (i.e. “the target server 104 determines that the request came from outside the security parameter”) [column 6 lines 48-49].

- “the client apparatus receives input of the second authentication information when a user instructs a connection request with respect to the connection server, calculates the first authentication information unique to the client apparatus again, looking into an association between the input second authentication information and the again calculated first authentication information by using the stored local authentication information, encrypting the second authentication information by a first encryption method to transmit to the authentication server the second authentication information encrypted by the first encryption method when it is concluded that the association is established” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].
- “the client apparatus receives the connection server address as the information guiding the connection destination from the authentication server, transmitting the second authentication information encrypted by a second encryption method to a connection server address, and starting a communication with the connection server” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].

but Subramaniam does not explicitly disclose,

- “the client apparatus calculates first authentication information unique to the client apparatus to register the first authentication information in the connection server preliminarily, and acquiring local authentication information associating the first authentication information with a predetermined second authentication information from the connection server to store the local authentication information”

However, Subramaniam does disclose,

- “a user name and password, the authentication information may include certificates, tokens, public keys, and/or data from authentication tools such as biometric scans, voice prints, retinal scans, fingerprint scans, magnetic card reader results, and so on. A wide variety of suitable authentication information is familiar to those of skill in the art”
[column 12 lines 40-46].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the applicant’s invention to include, “the client apparatus calculates first authentication information unique to the client apparatus to register the first authentication information in the connection server preliminarily, and acquiring local authentication information associating the first authentication information with a predetermined second authentication information from the connection server to store the local authentication information,” in Subramaniam’s invention for the purposes of authenticating a client/user using various forms of authentication procedures prior to permitting access.

Art Unit: 2109

Claim 13:

Subramaniam discloses a connection method using a network connection system including a client apparatus, an authentication server, and a connection server comprising,

- “storing by the authentication server a user name and a password, which are encrypted by a first encryption method, while associating the encrypted user name and the encrypted password with connection server address” (i.e. “the servers 104, 106 may also be configured by those of skill in the art in a wide variety of ways to operate as Internet servers, as intranet servers, as proxy servers, as directory service providers or name servers, as software component or other object servers, or as a combination thereof”) [column 5 lines 44-49].
- “transmitting by the client apparatus to the authentication server the user name and the password, which are encrypted by the first encryption method, together with a connection request” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].
- “receiving by the authentication server the connection request from the client apparatus” (i.e. “a redirector on the border server 106 redirects the request from the client 112 to the border server 106 during a step 122. The border server 106 is advertised as the target server”) [column 6 lines 61-64].

- “acquiring the user name and the password, which are encrypted by the first encryption method, as information identifying a user of the client apparatus, and a client address” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].
- “transmitting the acquired client address to the connection server address associated with the information identifying the user when the authentication server stores the information identifying the user” (i.e. “the external client 112 requests access to data which is stored on the target server... checking the IP address from which the request was made, communicating with the firewall software, or other familiar means”) [column 6 lines 42-48].
- “receiving by the connection server the client address of the client apparatus to be connected from the authentication server” (i.e. “the external client 112 requests access to data which is stored on the target server... checking the IP address from which the request was made, communicating with the firewall software, or other familiar means”) [column 6 lines 42-48].
- “allowing communication from the client apparatus” (i.e. “If the username and password are validated by the authentication system, the border server 106 so notifies the user, and the user is then granted access to secure network 100 data as described herein”) [column 8 lines 53-57].

- “encrypting a user name and a password, which are input by the user, by a second encryption method” (i.e. “a user name and password, the authentication information may include certificates, tokens, public keys, and/or data from authentication tools such as biometric scans, voice prints, retinal scans, fingerprint scans, magnetic card reader results, and so on. A wide variety of suitable authentication information is familiar to those of skill in the art”) [column 12 lines 40-46].
- “transmitting the user name and the password, which are encrypted by the second encryption method, to the connection server address received by the client server from the authentication server” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].
- “performing an authentication process by using the user name and the password, which are encrypted by the second encryption method and are received by the connection server from the client apparatus” (i.e. “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network”) [column 8 lines 50-53].

but Subramaniam does not explicitly disclose,

- “transmitting to the authentication server information indicating that the connection server is shifted to a connection wait state”

Art Unit: 2109

However, Subramaniam does disclose,

- “The user enters a user name and a corresponding password in fields shown on the login screen. The username and password are then transmitted over the secure connection to the border server 106, which passes them in turn to an authentication system within the secure network” [column 8 lines 50-53].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the applicant’s invention to include, “transmitting to the authentication server information indicating that the connection server is shifted to a connection wait state,” in Subramaniam’s invention since an authentication system would have to “wait” for the proper authentication information prior to permitting or denying a client/user from access resources.

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to the applicant’s disclosure.
 - a. Grantges (US-6324648-B1)
 - b. Liu (US-5898780-A)
 - c. Kingdon (US-5349642-A)
 - d. Shambroom (US-6301661-B1)
 - e. Ito (US-5671354-A)
 - f. Fritch (US-6105132-A)
 - g. Jin (US-6311275-B1)


Art Unit: 2109

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Myhre, can be reached at 571-270-1065. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
03/22/2007


James Myhre
Supervisory Patent Examiner